UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

RYOSUKE KONDO, individually and on behalf of themselves and all others similarly situated, Plaintiff, v. CREATIVE SERVICES, INC., Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Ryosuke Kondo ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint (the "Action") against Creative Services, Inc. ("Defendant" or "CSI"), a Massachusetts corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This Action arises out of the data breach (the "Data Breach") at CSI that targeted the information of employees who performed work for the entities that used CSI to provide background screening and security consulting for those same entities.

2. CSI is, according to its own website, "[t]he most trusted partner in background screening and security consulting."[1] Specifically, "[w]hat began as a small private investigation firm has evolved into a global, full-service employment screening and security consulting firm,

[1] https://www.creativeservices.com, (last accessed Mar. 10, 2022).

serving corporate, nuclear, and government market sectors."[2] CSI markets itself as having provided "45 years of service you can trust."[3]

3. However, Plaintiff Kondo and members of the putative Class had their trust violated and their privacy rights obscured due to CSI's failure to maintain necessary data security protocols.

4. The Data Breach resulted in unauthorized access to the sensitive data of employees of companies that used CSI's services. Because of the Data Breach, 164,673 Class Members' suffered ascertainable losses inclusive of out-of-pocket expenses and the value of their time incurred to remedy or mitigate the effects of the attack and the present risk of imminent harm caused by the compromise of their sensitive personal information, including financial account numbers, credit/debit card numbers (in combination with security code, access code, password or PIN for the respective account), name, date of birth, Social Security number, and/or driver's license number.

5. To compound matters, CSI first learned of the data breach (which occurred on November 23, 2021) on January 25, 2022. This means that CSI failed to monitor their networks to ascertain whether there were any intrusions, and failed to detect an intrusion for over two months – a critical failure of a company that lauds itself as "the most trusted partner in background and security screening."

6. Then CSI sat on the information for nearly a month – failing to disseminate data breach consumer notifications until February 23, 2022 and February 25, 2022, respectively. When a data set that is inclusive of the aforementioned personally identifiable information ("PII") is breached, every moment is precious to ensure that that data is not then weaponized against the rightful owner of that data through identity theft. Sitting on this information allowed CSI to dodge

[2] https://www.creativeservices.com/about, (last accessed, Mar. 10, 2022).
[3] *Id.*

responsibility and inevitably worsened the Data Breach victims' chances at weathering the storm that CSI created.

7. As a result of the Data Breach, Plaintiff and Class Members have been harmed – they have suffered actual fraud, and have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and forever in the future closely monitor their financial accounts to guard against identity theft.

8. Plaintiff and Class Members may also incur out-of-pocket costs, for example, through having to purchase credit monitoring systems, credit freezes, or other protective measures to deter and detect identity theft. Plaintiff seeks to remedy those harms on behalf of himself and all similarly situated persons whose PII was accessed unlawfully during the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement for out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

9. As such, Plaintiff brings this Action against Defendant seeking redress for its unlawful conduct, asserting claims for: (1) negligence, (2) unjust enrichment, and (3) violations of the Massachusetts Consumer Protection Law (Mass. Gen. Laws, Ch. 93a).

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act because (1) there are more than 100 putative Class members, (2) the aggregate amount-in-controversy, exclusive of costs and interest, exceeds $5,000,000.00, and (3) there is minimal diversity as required by the state because Plaintiff and Defendants are citizens of different states –

namely, that Plaintiff is a Colorado resident and the Defendant is headquartered here, in Massachusetts.

11. This Court has personal jurisdiction over the Defendant because the Defendant is from this District. Additionally, this Court has personal jurisdiction over the Defendant because they have substantial contacts with this District and have purposely availed themselves to the Courts in this District.

12. In accordance with 28 U.S.C. 1391, venue is proper in this District because a substantial part of the conduct giving rise to the Plaintiff's claims occurred in this District, the Defendant is headquartered in this District, and the Defendant transacts business within this District. In accordance with 28 U.S.C. § 1391, venue is proper in this District because a substantial part of the conduct giving rise to Plaintiff's claims occurred in this District and Defendant has intentionally availed themselves of the laws and markets within this District.

PARTIES

13. Plaintiff Ryosuke Kondo is, and at all times mentioned herein was, an individual citizen of Arvada, Colorado. Plaintiff was notified of the Data Breach and his Private Information being compromised upon receiving a data breach notification letter dated February 23, 2022.

14. Defendant CSI is a domestic corporation organized under the laws of the Commonwealth of Massachusetts with its principal place of business located at 64 Pratt Street, Mansfield, Massachusetts 02048.

FACTUAL ALLEGATIONS

Defendant's Business

15. Defendant CSI, founded approximately 45 years ago, is a background check and security screening solutions company. CSI has private investigator licenses, according to its website, in Massachusetts, South Carolina, the City of Providence, Rhode Island, and Connecticut.

16. According to CSI:

> CSI provides screening solutions that reduce client risk at all stages of the employment cycle. CSI's capabilities span from pre-hire options, such as assessment testing and applicant tracking, to traditional background screening services, drug testing, Electronic I-9 and E-Verify, and extend to post-hire solutions including periodic reinvestigations and annual checks. CSI also offers comprehensive vendor, contractor, and consultant screening solutions to reduce risk associated with extended workforces. Our programs include initial screening, adjudication programs, and program audits.[4]

17. Additionally, on the CSI website, it states:

> CSI maintains a strong commitment to best practices and innovative solutions. During our days as a private investigation firm, CSI recognized the need to address causation, prevention, and the importance of investigative techniques. We were a pioneer in background screening and today we continue to shape the future of our industry as we grow and pave the way for our clients' productive, safe hiring practices.[5]

18. The way that CSI works – at least with respect to subjects from contracting companies – is that CSI has both a standalone portal and a portal that is integrated into a contracting company's human resources platform (e.g. ADP, Oracle, Workable, Ceridian, etc.) and the subject inputs Personal Information into either the portal or into the H.R. platform. Then CSI collects that information and runs necessary and contracted testing (e.g. background checks, security

[4] https://www.creativeservices.com/about, (last accessed Mar. 15, 2022).
[5] *Id.*

authorizations, etc.) for the contracted company. Notably, some of the contracted companies are government entities.

19. Upon information and belief, and in the ordinary course of business conducting background checks and other security authorizations for contracting companies, CSI requires the following information from those same contracting companies on prospective hires and other types of subjects for background-type forensics:

i. Name

ii. Date of Birth

iii. Social Security number

iv. Driver's License number

20. Upon information and belief, CSI collects Personal Information from contracting companies from the following industries:

i. Biotechnology

ii. Cannabis

iii. Dietary Supplements

iv. Energy

v. Environmental Services

vi. Financial Services

vii. Healthcare

viii. Higher Education

ix. Life Sciences

x. Pharmaceuticals

xi. Technology

21. By obtaining, collecting, using and deriving benefits from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting said Private Information from unauthorized disclosure.

22. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

The Data Breach

23. To define data breaches: "a data breach exposes confidential, sensitive, or protected information to an unauthorized person. The files in a data breach are viewed and/or shared without permission."[6]

24. According to the Attorney General of Maine, on January 25, 2022, CSI discovered the Data Breach at-issue.[7]

25. The Data Breach itself took place on November 23, 2021, over two months after the Data Breach was discovered by CSI.[8] The breach, which was an external system breach (a/k/a hacking), was caused when an intruder penetrated CSI's systems.[9]

26. However, rather than promptly inform consumers about the seriousness and the dangers, which are well known, of data breaches – and of this particular Data Breach, specifically – the Defendant opted not to inform consumers until nearly a month after the discovery of the Data

[6] "*How Data Breaches Happen*," KASPERSKY, at https://www.kaspersky.com/resource-center/definitions/data-breach (last accessed Mar. 15, 2022).
[7] *See,* https://apps.web.maine.gov/online/aeviewer/ME/40/deb00156-358b-4bf5-80e1-cf0d189e9d3c.shtml (last accessed Mar. 15, 2022).
[8] *Id.*
[9] *Id.*

Breach on January 25, 2022.[10] Indeed, consumers were not notified that their data had been compromised until February 23, 2022 at earliest.[11]

27. This issue is compounded by the fact that CSI had a data breach only months prior – and released a data breach notification with respect to that earlier data breach on September 27, 2021.[12]

28. According to the Attorney General of Maine, information stolen in the Data Breach included "name or other personal identifier" in combination with credit/debit card number (inclusive of security code, access code, password, or PIN for that respective account).[13]

29. Further, according to the Notice of Data Privacy Incident letter sent to Plaintiff (dated February 23, 2022), the compromised information included Plaintiff's name and date of birth, Social Security number, and/or driver's license number.

30. The Private Information contained in the files accessed in the Data Breach were not encrypted.

31. Upon information and belief, the Data Breach was targeted at Defendant due to its rich trove of Personal Information collected from potential applicants for a wide range of potential industries.

32. While CSI stated in its "Notice" to consumers notifying them about the Data Breach that it learned of the Data Breach in January of 2022, CSI did not begin notifying impacted victims, such as Plaintiff and members of the putative Class, until February 23, 2022 – a month after discovering the Data Breach. CSI's delay in notifying the victims of the data breach violates provisions of the Massachusetts General Laws, Chapter 93H, and in particular, the reporting

[10] *Id*
[11] *Id.*
[12] *Id.*
[13] *Id.*

sections of c. 93H, Section 3, which required CSI, once it knew or had reason to know of a data security breach involving personal information of Massachusetts residents, to provide prompt and direct notice of such breach to any affected Massachusetts residents, the Massachusetts attorney general, and to the director of consumer affairs and business regulation for the Commonwealth of Massachusetts.

33. Plaintiff and Class Members provided their Private Information to Defendant with the reasonably expectation and the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. Defendant's data security obligations were particularly important given the substantial increase in data breaches preceding the date of the breach.

34. Therefore, the increase in such attacks, and the attendant risk of future attacks (especially by an entity like CSI that had been breached earlier in 2021) was widely known to the public and to anyone in the Defendant's industry, including the Defendant itself.

Defendant Fails to Comply with FTC Guidelines

35. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

36. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security

problems.[14] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[15]

37. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

38. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

39. Defendant failed to properly implement basic data security practices.

40. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

41. Defendant was at all times fully aware of its obligation to protect the PII of its subjects. Defendant was also aware of the significant repercussions that would result from its failure to do so.

---

[14] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Mar. 15, 2022).

[15] *Id.*

42. Several best practices have been identified that at a minimum should be implemented by companies like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

43. Other best cybersecurity practices that are standard in the Defendant's industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

44. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

45. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant's Breach

46. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer

systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches;

b. Failing to adequately protect consumers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train its employees in the proper handling of data breaches, the protection of Private Information, and the maintenance of adequate email security practices;

e. Failing to comply with the FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and,

f. Failing to adhere to industry standards for cybersecurity.

47. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access CSI's IT systems which contained unsecured and unencrypted Private Information.

48. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and Class Members also lost the benefit of the bargain they made with Defendant.

Harm to Consumers

49. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

50. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

51. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

52. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

53. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

54. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[16]

[16] Brian Naylor, "*Victims of Social Security Number Theft Find It's Hard to Bounce Back*," NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

55. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[17]

17. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you.
>
> Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[18]

18. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[19] However, this is not the case. As cybersecurity experts point out:

> It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks.[20]

19. Victims of driver's license number theft also often suffer unemployment benefit

---

[17] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed July 20, 2021).

[18] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?"* (October 24, 2018) https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last accessed July 20, 2021).

[19] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed July 20, 2021).

[20] *Id.*

fraud, as described in a recent New York Times article.[21]

20. The fraudulent activity resulting from the Data Breach may not come to light for years.

21. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

22. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, driver's license numbers, and financial account information, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

56. Defendant knew or should have known about these dangers and strengthened its data, IT, and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

---

[21] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed July 20, 2021).

[22] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 19, 2022).

Harm to Plaintiff

57. Plaintiff Ryosuke Kondo is a resident and citizen the State of Colorado and intends to remain domiciled in and a citizen of the State of Colorado.

58. Plaintiff Kondo received a letter dated February 23, 2022 from Defendant concerning the Data Breach. The letter stated that his name and date of birth, Social Security number and/or driver's license number were included in the Data Breach.

59. Upon information and belief, Plaintiff Kondo's email address provided to Defendant was also compromised in the Data Breach.

60. The Notice of Data Privacy Incident letter received by Plaintiff Kondo specifically instructed him to spend time mitigating the effects of the Data Breach, including time spent "reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors," spending time enrolling in credit monitoring services, and spending time reviewing a publication entitled "Steps You Can Take to Help Protect Your Personal Information."

61. As a result of the Data Breach, Plaintiff has suffered actual fraud, in that a cybercriminal fraudulently opened (or attempted to open) an account at Best Buy in Plaintiff's name. Plaintiff was forced to expend time dealing with the effects of this fraud.

62. As a result of the Data Breach, Plaintiff has suffered emotional distress as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including increased anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach. Plaintiff Kondo is also worried that his family members may

be affected, as the address that the Data Breach Notification Letter was sent to is not his address – it is his parents' address.

63. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that CSI obtained from Plaintiff; (b) violation of his privacy rights; (c) present injury in the form of fraud or attempted fraud using the information compromised in this Data Breach, and (d) present injury arising from the increased and imminent risk of identity theft and fraud.

64. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff will continue to be at increased risk of identity theft and fraud for years to come.

65. Specifically, Plaintiff Kondo is cognizant of security and does take affirmative steps to protect his data privacy – such as, using 2-factor authentication and taking careful steps to delete files that contain personal information in them, especially personal information that is derived from data.

66. Plaintiff Kondo, since the onset of the Data Breach, has taken steps to monitor his financial accounts, his credit monitoring reports (which required him calling Experian and having records corrected). He estimates that he has spent 2 to 3 hours of time, including time spent calling the Defendant's helpline, which Plaintiff Kondo found "helpless."

67. Plaintiff's Private Information was compromised as a direct and proximate result of the Data Breach.

68. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

69. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

70. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

71. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

CLASS ALLEGATIONS

72. Plaintiff brings this Action on behalf of himself and on behalf of all other persons similarly situated (the "Class"). Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons who utilized CSI's services, whose Private Information was maintained on CSI's system that was compromised in the Data Breach, and who were sent a notice of the Data Breach (the "Class Definition").

73. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Also excluded from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

74. **Numerosity**. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of over 100,000 individuals whose sensitive data was compromised in the Data Breach.

75. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether the Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to, during, and after the Data Breach complied with the applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards, as applicable;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached a duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members Private Information in the Data Breach;

h. Whether the Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether the Plaintiff and Class Members suffered legally cognizable injuries as a result of the Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

l. Whether Defendant failed to provide notice of the Data Breach in a timely manner;

m. Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief;

76. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

77. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.

78. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

79. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

80. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CAUSES OF ACTION

COUNT ONE

Negligence

81. Plaintiff re-alleges and incorporates by reference each of the preceding paragraphs as if fully set forth herein.

82. Defendant required consumers, including Plaintiff and Class Members, to submit non- public Private Information in the ordinary course of rendering services.

83. By collecting and storing this data in its computer property, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to

prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

84. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

85. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its consumers. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

86. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

87. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

88. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement and maintain adequate security measures to safeguard Class Members Private Information;

b. Failing to adequately monitor the security of its IT systems;

c. Failing to ensure that its email systems had plans in place to maintain reasonable data security safeguards;

d. Failure to have in place mitigation policies, strategies, and procedures;

e. Allowing unauthorized access to Class Members Private Information; and,

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate measures to mitigate the potential for identity theft and other damages.

89. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches, and the prior data breach involving Defendant.

90. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

91. Plaintiff and Class Members suffered injury and damages as a result of the Defendant's negligence, as outlined above.

92. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

93. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit

to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT TWO

Unjust Enrichment

94. Plaintiff re-alleges and incorporates by reference each of the preceding paragraphs as if fully set forth herein.

95. Plaintiff and Class Members conferred a monetary benefit on CSI in the form of monetary payments—made to CSI directly or indirectly—from the companies (like Plaintiff's prior employer – The Charles Stark Draper Laboratory) that use CSI's services in order to perform various screenings.

96. CSI collected, maintained, and stored the PII of Plaintiff and Class Members and, as such, Defendant CSI had knowledge of the monetary benefits conferred by the companies that use CSI's services (like Plaintiff's prior employer Draper Laboratory) on behalf of the Plaintiff and Class Members.

97. The money that companies that use CSI's services (like Draper Laboratory) paid to CSI should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII.

98. Defendant CSI failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

99. As a result of Defendant CSI's failure to implement data security practices, procedures, and programs to secure sensitive PII, Plaintiff and Class Members suffered actual

damages in an amount of the savings and costs Defendant CSI reasonably and contractually should have expended on data security measures to secure Plaintiff's PII.

100. Under principles of equity and good conscience, Defendant CSI should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant CSI failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII and that CSI customers like Draper Laboratories (Plaintiff's former employer) paid for.

101. As a direct and proximate result of Defendant CSI's decision to profit rather than provide adequate security, and Defendant CSI's resultant disclosures of Plaintiff and Class Members' PII, Plaintiff and Class Members suffered and continue to suffer considerable injuries in the forms of attempted identity theft, time and expenses mitigating harms, diminished value of PII, loss of privacy, and an increased risk of harm.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiff and his counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised by the Data Breach.

JURY TRIAL DEMAND

Jury trial is demanded by Plaintiff and members of the putative Class.

DATED: March 22, 2022

Respectfully submitted,

s/ *Douglas F. Hartman*
Douglas F. Hartman, BBO# 642823
HARTMAN LAW, P.C.
10 Post Office Square
Suite 800 South
Boston, Massachusetts 02109
T: 617-807-0091
F: 617-507-8334
dhartman@hartmanlawpc.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Attorneys for Plaintiff and the Proposed Class

**Pro hac vice applications forthcoming*